UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,809	12/11/2000	Messaoud Benantar	AUS9-2000-0799-US1	2057

7590 06/17/2004

Joseph R. Burwell
Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, TX 78755-8022

EXAMINER
VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
2131	5

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/734,809	**Applicant(s)** BENANTAR, MESSAOUD	
	Examiner Michael R Vaughan	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 December 2000* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 1-32 have been examined and are pending.

Information Disclosure Statement

An initialed and dated copy of Applicant's IDS form 1449, Paper No. 4, is attached to the instant Office action.

Claim Rejections - 35 USC ' 103

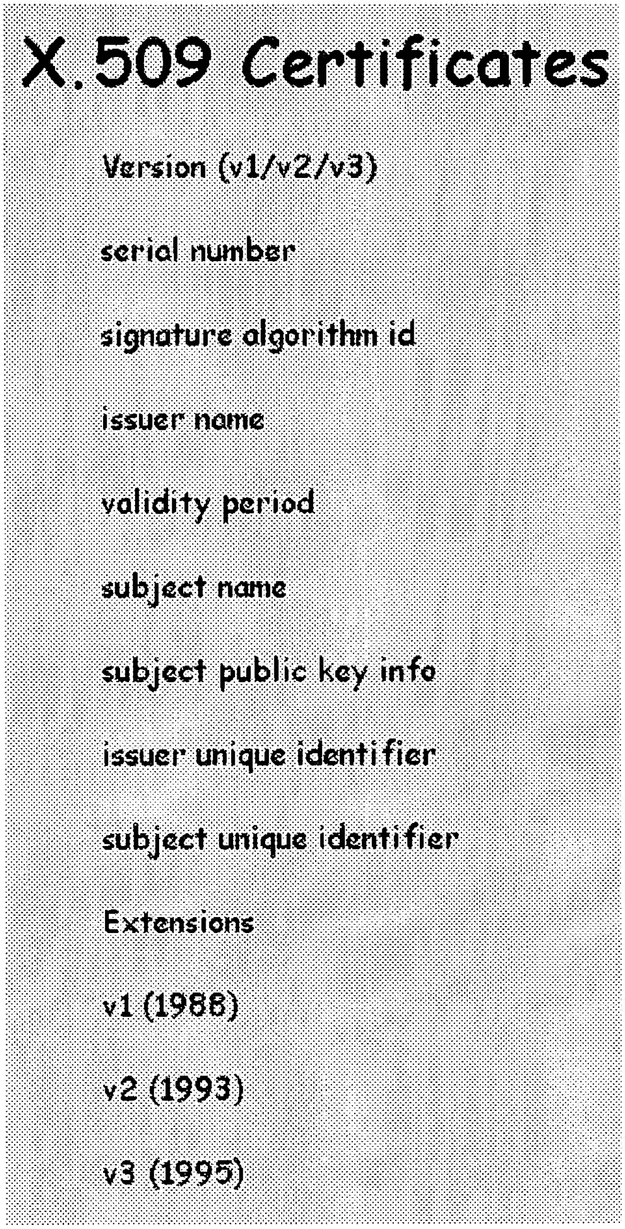
The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject

> matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al, hereinafter, Van Oorschot (USP 5,699,431) in view of RFC 2459, Internet X.509 Public Key Infrastructure.

As per claims 1, 11, and 21, Van Oorschot teaches a method for validating a digital certificate within a data processing system, the method comprising: receiving a digital certificate (col. 1, line 50); retrieving a certificate revocation list (col. 1, line 61-62); extracting a first serial number from the digital certificate, wherein the first serial number has been associated with the digital certificate by a certifying authority (col. 2, lines 7-8); determining whether the first serial number matches a second serial number stored (col. 2, line 8) within the certificate revocation list. Van Oorschot teaches that a match in the serial number means that the certificate has been revoked. Van Oorschot teaches that in the certificate is option information that specifies where additional access information about certificate may be found (col. 2, lines 56-63). One type of additional access information as disclosed by Van Oorschot is the particular CA that was used to certify that particular certificate (col. 5, lines 13-24). Van Oorschot's system can be applied to the X.509 standard of digital certificates. Here is the format of a X.509 certificate:



X.509 Certificates

Version (v1/v2/v3)

serial number

signature algorithm id

issuer name

validity period

subject name

subject public key info

issuer unique identifier

subject unique identifier

Extensions

v1 (1988)

v2 (1993)

v3 (1995)

Van Oorschot teaches computing a first certificate fingerprint for the digital certificate (col. 5, lines 39-40). Van Oorschot does not explicitly teach comparing the first certificate fingerprint with a second certificate fingerprint stored within the certificate revocation list, wherein the second certificate fingerprint is associated with the second serial number. RFC 2459 states on page 23 that:

> "**4.1.2.8 Unique Identifiers**
>
> These fields may only appear if the version is 2 or 3 (see sec. 4.1.2.1). The subject and issuer unique identifiers are present in the certificate to handle the possibility of reuse of subject and/or issuer names over time."

From the format of the X.509 certificate one of ordinary skill in the art would know that the additional information included in the certificate of Van Oorschot to identify a particular CA is essentially an issuer unique identifier. As stated by RFC 2459, this optional field is used to avoid ambiguousness of CA over time. In fact both the issuer and subject unique identifiers are designed to avoid conflicts of possible reuse of an issuer or subject name. Therefore both fields represent fingerprinting data because they provide uniqueness. Van Oorschot teaches that this value can be embedded in a certificate (col. 5, lines 39-40) and that it should be verified (col. 2, lines 59-61). It would then be advantageous to match this optional information, which the additional information stored at the CRL, similarly to how the serial numbers are matched. Further evidence of matching is suggested by Van Oorschot teaches that the additional information is also kept at a secondary location (one other than on the certificate itself) (col. 4, lines 5-7). To summarize, based on the optional fields of the X.509 standard, it would have been obvious to use the additional access information taught by Van Oorschot as a further matching/verification parameter to determine if a certificate is revoked.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of RFC 2459 within the system of

Van Oorschot because it would prevent ambiguousness of certificates in the event that names were reused by the certificate authority.

As per claims 7, 17, and 27, Van Oorschot teaches receiving a serial number for a digital certificate, wherein the serial number has been associated with the digital certificate by a certifying authority (col. 2, lines 6-8); creating an entry in a certificate revocation list for the digital certificate (col. 1, lines 50-60), wherein the entry comprises the serial number for the digital certificate (col. 2, lines 7-8); computing a certificate fingerprint for the digital certificate (col. 5, lines 38-40). Van Oorschot does not explicitly teach storing the certificate fingerprint within the entry in the certificate revocation list for the digital certificate. Van Oorschot teaches that this value can be embedded in a certificate (col. 5, lines 39-40) and that it should be verified (col. 2, lines 59-61). It would then be advantageous to match this optional information, which the additional information stored at the CRL, similarly to how the serial numbers are matched. Further evidence of matching is suggested by Van Oorschot teaches that the additional information is also kept at a secondary location (one other than on the certificate itself) (col. 4, lines 5-7). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Van Oorschot by also storing the fingerprint data at the CRL because he teaches that it must be verified. The digital certificates are validated by the CA, which uses the CRL to make the determination. The examiner supplies the same rationale for the motivation as recited in the rejection of claim 1 to incorporate the teachings of RFC 2459 to use the unique issuer identifier to avoid ambiguousness in serial number and CA names. One of ordinary skill in the art would then use the unique issuer identifier (fingerprint) in conjunction with the serial numbers to certify. It would have been obvious to one of ordinary skill in the art at the time of the invention to keep both a copy of the unique issuer identifier and serial number in the CRL.

As per claims 2, 12, and 22 the examiner supplies the same rationale for the motivation to modify the teaching Van Oorschot by using the unique issuer identifier field to make a comparison with locality information stored at the CRL. From this modification it logically follows that if the serial numbers and the unique issuer identifier (fingerprint) matches the record in the CRL then the certificate will be revoked.

As per claims 3, 13, and 23 similar to claim 2, once modifying the system of Van Oorschot, if the fingerprinting data does not match that of the record data, the CA would then certify the certificate because that certificate had not been previously revoked.

As per claims 4, 8, 14, 18, 24, and 28,Van Oorschot teaches the digital certificate and the certificate revocation list are formatted according to the X.509 standard (col. 1, lines 49-50).

As per claims 5, 9, 15, 19, 25, and 29 Van Oorschot teaches the second certificate fingerprint is stored within an X.509 extension within the certificate revocation list (col. 1, lines 49-50).

As per claim 6, 10, 16, 20, 26, and 30, Van Oorschot teaches the step of computing a first certificate fingerprint for the digital certificate uses a digest algorithm in accordance with a digest algorithm identifier stored in association with the second certificate fingerprint (col. 5, lines 38-41). Also X.509 standard includes this algorithm identifier field.

As per claims 31 and 32, Van Oorschot teaches a data structure representing a certificate revocation list for use in a data processing system, the data structure comprising: a serial numbers of a revoked digital certificates (col. 2, lines 1-8 and col. 1, lines 49-51). The examiner supplies the same rational for the motivation as recited in the rejection of claim 1 to incorporate the teachings of RFC 2459 within the system of Van Oorschot to include a copy of the certificate fingerprint for the revoked digital certificate at the CRL.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan

Examiner

Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100